Amendments to the Claims

1. (CURRENTLY AMENDED) A method of performing a reduction operation in a cryptographic calculation, the method comprising selecting a modulus having a first section with a plurality of "1" Most 8ignificant Word states and a second section which comprises a, plurality of "1" or "0" states whereby the number formed of the two sections is a modulus or a multiple of a modulus, and operating ~~(S1-S5; S10-S12; S20-S26)~~ a reduction operation on the modulus/multiple.

2. (CURRENTLY AMENDED) A method according to Claim 1 comprising effecting a plurality of multiplication operations ~~(S1)~~.

3. (CURRENTLY AMENDED) A method according to Claim 2 comprising effecting a plurality of multiplication operations followed by effecting a reduction operation ~~(S1, S2)~~.

4. (CURRENTLY AMENDED) A method according to Claim 3 comprising repeating the combined multiplication operations and reduction operation ~~(S1, S2)~~.

5. (CURRENTLY AMENDED) A method according to ~~any preceding claim~~Claim 1 comprising using a multiple of the modulus/multiple.

6. (CURRENTLY AMENDED) A method according to ~~any preceding claim~~Claim 1 wherein, when the last multiplication gives an overflow ~~(S4)~~, the overflow is added to a part of the selected number.

7. (CURRENTLY AMENDED) A method according to Claim 6 wherein, when the overflow addition step ~~(S4)~~ produces an overflow, then n_0' ~~(S5)~~ is added to the overflow.

8. (CURRENTLY AMENDED) A method according to ~~any preceding claim~~Claim 1, wherein the carry c between two adjacent multiplications is effected as the addend in the next multiplication~~(S2)~~.

9. (CURRENTLY AMENDED) A method according to ~~any preceding claim~~Claim 1 comprising monitoring the number of leading "1"s to determine if the number is less than (k-2).

10. (CURRENTLY AMENDED) A method according to Claim 6 comprising initiating the next calculation when the number of leading "1"s is less than (k-2).

11. (CURRENTLY AMENDED) A method according to ~~any preceding claim~~Claim 1 the method comprising operating 192-bit ECC and a word size of 64-bit, the modulus comprises a first section of 138 bits and a second section of 54 bits.

12. (CURRENTLY AMENDED) A method according to ~~any of Claims 1 to 10~~Claim 1 the method comprises operating 128-bit ECC and a word size of 64-bit, the modulus comprises a first section of 74 bits and a second section of 54 bits.

13. (CURRENTLY AMENDED) A method according to ~~any of Claims 1 to 10~~Claim 1 the method comprising operating 256-bit ECG and a word size of 54-bit, the modulus comprises a first section of 202 bits and a second section of 54 bits.

14. (CURRENTLY AMENDED) A computer program product directly loadable into the internal memory of a digital computer, comprising software code portions for performing the method of ~~anyone or more of Claims 1 to 13~~Claim 1 when said product is run on a computer.

15. (CURRENTLY AMENDED) A computer program directly load able into the internal memory of a digital computer, comprising software code portions for performing the method of ~~anyone or more of Claims 1 to 13~~Claim 1 when said

program is run on a computer.

16. (ORIGINAL) A carrier, which may comprise electronic signals, for a computer program of Claim 15.

17. (ORIGINAL) Electronic distribution of a computer program product of Claim 14 or a computer program of Claim 15 or a carrier of Claim 16.

18. (CURRENTLY AMENDED) Apparatus for performing a reduction operation in a cryptographic calculation, the apparatus comprising means to select a modulus or a multiple of a modulus having a first section with a plurality of "1" states and a second section having a plurality of "1" or "0" states whereby the number formed of the two sections is a modulus or a multiple of a modulus, and means ~~(10-17)~~ for operating a reduction operation on the modulus/multiple.

19. (CURRENTLY AMENDED) Apparatus according to Claim 18 comprising means ~~(10-17)~~ to effect a plurality of multiplication operations.

20. (CURRENTLY AMENDED) Apparatus according to Claim 19 comprising means ~~(10-17)~~ to effect a plurality of multiplication operations followed by a reduction operation.

21. (CURRENTLY AMENDED) Apparatus according to Claim 20 comprising means ~~(10-17)~~ to repeat the combined multiplication operations and reduction operation.

22. (CURRENTLY AMENDED) Apparatus according to ~~any of Claims 18-21~~Claim 18 comprising means (10-17) to use a multiple of the modulus/multiple.

23. (CURRENTLY AMENDED) Apparatus according to ~~any of Claims 18 to 22~~Claim18 comprising means ~~(10-17)~~, when the last multiplication gives an overflow, to add the overflow to a part of the selected number.

24. (CURRENTLY AMENDED) Apparatus according to Claim 23 comprising means~~(10-17)~~, when the overflow addition step produces an overflow, to add n_0' to the overflow.

25. (CURRENTLY AMENDED) Apparatus according to ~~any of Claims 18 to 24~~Claim 18 ~~(10-17)~~comprising means to effect the carry c between two adjacent multiplications as the addend in the next multiplication.

26. (CURRENTLY AMENDED) Apparatus according to ~~any of Claims 18 to 25~~Claim 18 ~~(10-17)~~comprising means to monitor the number of leading "1"s to determine if the number is less than (k-2).

27. (CURRENTLY AMENDED) Apparatus according to ~~any of Claims 18 to 26~~Claim 18 comprising means ~~(10-17)~~to initiate the next calculation when the number of leading "1"s is less than (K-2).

28. (CURRENTLY AMENDED) Apparatus according to ~~any of Claims 18 to 27~~Claim 18 with means ~~(10-17)~~ for 192-bit EEC and a word size of 64-bit, the modulus comprises a first section of 74 bits and a second section of 54 bits.

29. (CURRENTLY AMENDED) Apparatus according to ~~any of Claims 18 to 27~~Claim 18 with means ~~(10-17)~~for 128-bit ECC and a word size of 64-bit, the modulus comprises a first section of 74 bits and a second section of 54 bits.

30. (CURRENTLY AMENDED) Apparatus according to ~~any of Claims 18 to 27~~Claim 18 with means, ~~(10-17)~~for 256-bit ECC and 81 word size of 64-bit, the modulus comprises 81 first section of 202 bits and 81 second section of 54 bits.

31. (ORIGINAL) A method of performing a reduction operation substantially as hereinbefore described with reference to, and/or as illustrated in, anyone or more of Figures 1 to 5 of the accompanying drawings.

32. (ORIGINAL) Apparatus for performing a reduction operation in a

cryptographic calculation, the apparatus substantially as hereinbefore described with reference to, and/or as illustrated in, anyone or more of Figures 1 to 5 of the accompanying drawings.

33. (ORIGINAL) A method of performing a reduction operation in a cryptographic calculation, the method substantially as hereinbefore described with reference to, and/or as illustrated in, anyone or more of Figures 1 to 5 of the accompanying drawings.